CS4677 Computer Forensics Web & E-mail Analysis

Chris Eagle

Spring '06

References

- Textbook
  - Chapter 10
    - Browser cache investigation
  - Chapter 11
    - E-mail activity reconstruction
  - Chapter 21
    - Tracing E-mail

Web Activity

- Book discusses IE index.dat files
  - Introduces tools to parse IE data files
  - Useful to learn original URL that file came from
- Mozilla/Firefox
  - Need to find users Cache directory
  - about:cache
  - Use *file* command to identify
- M time – initial download
- A time – last access

Cookies

- Affiliated with particular web site
- Name/Value pair
- Most have expiration time
- IE cookies store creation time
- Browser cookie viewer along with raw dump of cookie file will help you decipher cookie file format

Viewing Email

- Book details various commercial and open source tools
- Easiest solution
  - Use the application that created the data
  - Use different application capable of importing your data
  - Use specialized utilites
    - pst2mbox
    - libPST
  - strings

Tracking E-mail

- Each mail server in chain adds a “Received” header indicating IP address of previous mail server
- Only last (topmost) Received header can be trusted
- Many webmail services add a header containing the originators IP
  - Circumvented by anonymous remailers